UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,937	08/20/2001	Masahiro Kaminaga	NITT.0027	4651

38327 7590 05/12/2005

REED SMITH LLP
3110 FAIRVIEW PARK DRIVE, SUITE 1400
FALLS CHURCH, VA 22042

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/931,937	**Applicant(s)** KAMINAGA ET AL.	
	Examiner Minh Dinh	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 2/17/2005. Claims 1-12 have been amended. The abstract has also been amended.

Response to Arguments

2. Applicant's arguments filed 2/17/2005 have been fully considered but they are not persuasive. Independent claims 1, 5 and 9 have been amended such that the methods in the originally filed claims are now performed by an IC card. However, the added feature has already been addressed in the rejections of dependent claims 4, 8 and 12 under 35 USC 103 in the previous Office action.

In response to applicant's argument that that Blanchard (6,219,791) teaches detecting errors accidentally made during encryption/decryption, but not errors "internationally" generated by an IC card attacker (the word "internationally" is considered a typo error and is understood as "intentionally", see Specification p. 3, line 25). It is noted that the feature is not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant argues that Boneh ("On the Importance of Checking Cryptographic Protocols for Faults") does not teach any tamper-resistant (defending/protecting) fault detection method for an IC card, and therefor, teaches a way from the invention (p. 10, 1st paragraph). Boneh does teach that a smart card using RSA to generate signatures should check that the correct signature has indeed been produced to prevent attacks on the smart cards using induced hardware faults (p. 37, last par; p. 38, 4th par).

Applicant argues that Daniels (5,991,401) does not disclose controlling the output of the processing result Z and outputting it when it is correct (p. 10, last paragraph). Daniels teaches this feature in steps 43-45 of figure 3.

Regarding the features relied upon and reasons for using the references Fernandez-Gomez ("Concurrent Error Detection in Block Ciphers"), Ogg (US 2002/0178354 A1), and Schneier ("Applied Cryptography"), please refer to the corresponding rejections in the previous Office Action.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard et al. (6,219,791) in view of Boneh et al. ("On the Importance of Checking Cryptographic Protocols for Faults"). Blanchard discloses a method for verifying the result of a cryptographic operation using an information processing device comprising the steps of: performing a symmetric-key encryption process in which a secret key K is to be applied to an input plaintext M, and storing a processing result Z in a memory (fig.

4, step 420; fig. 1, elements 12, 20 and 30); performing a corresponding decryption process for said processing result Z on said memory and storing the decryption result W on the memory (fig. 4, step 430; fig. 1, element 30); outputting said processing result Z from said information processing device when said processing result W coincides with said plaintext M (fig. 4, step 470); and suppressing the output of said processing result Z from said information processing device when said processing result W does not coincide result when with said plaintext M (fig. 4, step 480).

Blanchard does not disclose an IC card performing the method of claim 1 to verify a cryptographic process. Boneh discloses a smart card verifying the correctness a cryptographic computation to prevent attacks on the smart card using induced hardware faults (p. 37, last par; p. 38, 4th par). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Blanchard method such that it is implemented on a smart card, as taught by Boneh. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

5. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard in view of Boneh as applied to claim 1 above, and further in view of Fernandez-Gomez et al. ("Concurrent Error Detection in Block Ciphers"). Blanchard discloses using a symmetric-key algorithm (fig. 1). Blanchard does not disclose using DES algorithm. Fernandez-Gomez discloses using DES algorithm (p. 980, right col., "The technique proposed ... in section 4"). It would have been obvious to one of ordinary skill in the art

at the time the invention was made to modify the combined method of Blanchard and Boneh to use DES algorithm, as taught by Fernandez-Gomez. The motivation for doing so would have been that DES is a current and widely used encryption algorithm.

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blanchard in view of Boneh as applied to claim 1 above, and further in view of Ogg et al. (US 2002/0178354 A1). Blanchard does not disclose that the device is reset. Ogg discloses a cryptographic device being reset in response to an attack (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Blanchard and Boneh such that the device is reset in response to an attack, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

7. Claims 5-6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels et al. (5,991,401) in view of Fernandez-Gomez and Boneh. Daniels discloses a method for verifying the result of a cryptographic operation using an information processing device comprising the steps of: performing a decryption process wherein a master key is to be applied to an input ciphertext C, and storing a processing result Z in a memory (fig. 3, step 41); performing an encryption process for said processing result Z on said memory using an encryption key, and storing the result W on the memory (fig. 3, step 42); outputting said processing result Z from the information processing device when said processing result W coincides with said ciphertext C (fig.

3, step 44); and suppressing the output of said processing result Z from the information processing device when said processing result W does not coincide result when with said ciphertext C (fig. 3, step 45).

Daniels does not disclose using a symmetric algorithm. Fernandez-Gomez discloses using DES, which is a symmetric algorithm (p. 980, right col., "The technique proposed ... in section 4"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method to use DES algorithm, as taught by Fernandez-Gomez. The motivation for doing so would have been that DES is a current and widely used encryption algorithm. Accordingly, the same key is used in both encryption and decryption processes.

Daniels does not disclose an IC card performing the method of claim 5 to verify a cryptographic process. Boneh discloses a smart card verifying the correctness a cryptographic computation to prevent attacks on the smart card using induced hardware faults (p. 37, last par; p. 38, 4th par). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method further such that it is implemented on a smart card, as taught by Boneh. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels, Fernandez-Gomez and Boneh as applied to claim 5 above, and further in view of Ogg. Daniels does not disclose that the device is reset. Ogg discloses a cryptographic

device being reset in response to an attack (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels, Fernandez-Gomez and Boneh such that the device is reset in response to an attack, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

9. Claims 9-10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels in view of Schneier ("Applied Cryptography") and Boneh. Daniels discloses a method for verifying the result of a cryptographic operation using an information processing device comprising the steps of: performing a decryption process wherein a master key is to be applied to an input ciphertext C, and storing a processing result Z in a memory (fig. 3, step 41); performing an encryption process for said processing result Z on said memory using an encryption key, and storing the result W on the memory (fig. 3, step 42); outputting said processing result Z from the information processing device when said processing result W coincides with said ciphertext C (fig. 3, step 44); and suppressing the output of said processing result Z from the information processing device when said processing result W does not coincide result when with said ciphertext C (fig. 3, step 45).

Daniels does not disclose using the RSA algorithm. Schneier discloses using RSA algorithm (Section 19.3, p. 466-467, "Soon after Merkle's knapsack ... confidence level in the algorithm"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method to use RSA algorithm, as taught by Schneier. The motivation for doing so would have been that RSA is the easiest to understand and implement of all public-key algorithms. Accordingly, the same key is used in both encryption and decryption processes.

Daniels does not disclose an IC card performing the method of claim 5 to verify a cryptographic process. Boneh discloses a smart card verifying the correctness a cryptographic computation to prevent attacks on the smart card using induced hardware faults (p. 37, last par; p. 38, 4th par). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Daniels method further such that it is implemented on a smart card, as taught by Boneh. A smart card needs to verify the correctness a cryptographic computation to prevent the danger that hardware faults poses to various cryptographic protocols.

10. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniels, Schneier and Boneh as applied to claim 9 above, and further in view of Ogg. Daniels does not disclose that the device is reset. Ogg discloses a cryptographic device being reset in response to an attack (par. 0042). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Daniels, Fernandez-Gomez and Boneh such that the device is reset in response to an attack, as taught by Ogg. The motivation for doing so would have been to protect against attempts to retrieve critical information.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
5/9/2005

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100